L'ESPIONNAGE ECONOMIQUE, NOUVEAU MOYEN DE PUISSANCE ETATIQUE ?

Mémoire de géopolitique

du chef de bataillon Hubert GOMART

dans le cadre du séminaire « géopolitique et économie »

Directeur : Christian HARBULOT

Mars 2006

FICHE DOCUMENTAIRE

1. Espionnage économique, un nouveau facteur de puissance étatique ?
2. 2006_memoire_geop_espionnage économique_Gomart
3. Chef de bataillon, armée de Terre, GOMART Hubert, France
4. 22 mars 2006
5. Division A – groupe A3
6. Mémoire de géopolitique
7. A travers la mondialisation des échanges, l'information devient l'enjeu de domination économique. Pour atteindre les objectifs inhérents à la quête de cette domination, les dérives vers l'espionnage industriel ne sont pas rares et pourraient s'apparenter à un véritable pillage économique de l'adversaire. Mais les informations « noires » ou « fermées », celles gardées jalousement secrètes, prennent une valeur inestimée pour le moment, conférant à ceux-là même qui les détiennent le statut de puissance.
8. intelligence économique – espionnage industriel – patriotisme économique – information – investissement étranger – patrimoine – lobbying – fusion – acquisition – souveraineté – puissance immatérielle – veille économique – agent d'influence -

SOMMAIRE

PREMIÈRE PARTIE : LE TRAITEMENT DE L'INFORMATION, ENJEU DE LA GUERRE ECONOMIQUE

Le rôle stratégique de l'information

L'information, arme de domination économique

Pouvoir et manipulation de l'information

Capter l'information par un système de veille

De l'intelligence économique à l'espionnage industriel

DEUXIÈME PARTIE: L'ESPIONNAGE INDUSTRIEL OU L'ORGANISATION DU PILLAGE ECONOMIQUE

Les fondements de l'espionnage industriel

Moyens et procédés de l'espionnage industriel

Les acteurs et les cibles

Des espions non inquiétés

La protection du patrimoine de l'entreprise

La protection offensive

TROISIÈME PARTIE: L'INFORMATION FERMEE, FACTEUR DE PUISSANCE

Le lobbying, agent d'influence et de pouvoir

Fusions ou acquisitions imposées

Les investissements étrangers face à la notion de patrimoine économique

Puissance immatérielle : une menace sur la souveraineté des Etats

INTRODUCTION

Là où la guerre froide l'avait confiné dans un face-à-face entre services de contre-espionnage, le renseignement retrouve aujourd'hui toutes ses dimensions : connaissance des acteurs et des stratégies (renseignement extérieur), détection des menaces (contre espionnage et contre-terrorisme), influence indirecte sur les situations (action secrète). C'est pourquoi cette activité nécessairement secrète et souvent méprisée est maintenant considérée par certains, dont monsieur le préfet R. Pautrat[1], comme un des "nouveaux moyens de la puissance".
Cette nouvelle exigence du renseignement est ressentie non seulement par les États mais elle est aussi partagée par les entreprises privées qui développent leur gestion stratégique et leur capacité d'influence globale.

Les pratiques de "business intelligence" très développées outre-Atlantique mêlent différents aspects des pratiques d'entreprise **:** la veille technologique, la sécurité industrielle, la propriété intellectuelle, le traitement électronique des données, l'usage de l'Internet,… En France, le rapport Martre pour le Plan en 1994, a donné à cette nouvelle activité une appellation à multiples sens : l'"intelligence économique". Les objectifs en sont ambitieux, qu'il s'agisse d'ouvrir les acteurs privés aux pratiques de traitement de l'information issues des services d'État (l'"Intelligence" anglosaxonne) pour mieux les protéger contre les risques d'espionnage industriel ou, simplement, de rendre les stratégies économiques plus intelligibles afin que les entreprises soient plus anticipatrices et moins réactives.

L'activité traditionnelle du renseignement était centrée sur la recherche par des moyens occultes d'informations secrètes. Aujourd'hui le principal défi réside dans la capacité à trier et à croiser les données pertinentes parmi l'ensemble des informations ouvertes disponibles. Dans un environnement mondialisé et fortement concurrentiel, la maîtrise de l'information joue un rôle déterminant dans les prises de décision destinées à conquérir de nouveaux marchés. Tous les coups sont permis dans la guerre que se livrent les entreprises ou les Etats pour s'approprier des renseignements ciblés sur les concurrents, les secteurs dits stratégiques, les technologies. C'est une guerre silencieuse, un conflit étouffé, qui fait de nombreuses victimes (chômeurs, exclus de la société…). Les fondements mêmes des sociétés en sont affectés. Les entreprises constituent les principaux acteurs de cette guerre économique dans laquelle elles s'affrontent avec ou sans la complicité des Etats. Des guerriers en col blanc se jouent des règles commerciales, se moquent de l'éthique et n'ont qu'une religion : l'augmentation des marges.

---

[1] R. Pautrat : ancien directeur de la DST, "Le renseignement aujourd'hui ou les nouveaux moyens de la puissance", *Le Débat*, janvier-février 1992

L'information est donc plus que jamais devenue une denrée indispensable, dont on ne mesure le prix que quand on ne la possède pas. Car l'information c'est du temps de gagné. Il s'agit en effet d'améliorer sa réactivité et sa compétitivité par la connaissance de ce que fait la concurrence. Cela passe par la recherche, l'évaluation et la production d'informations élaborées, qui influenceront par exemple la définition d'une politique de développement ou bien la détermination de nouvelles orientations stratégiques.
En corollaire, bien évidemment, il faut savoir protéger son information, en maîtriser la diffusion et ne pas faciliter le travail des concurrents ou des bureaux spécialisés par manque de discrétion, de vigilance ou tout simplement de bon sens. Ainsi, par bavardages inconsidérés sur l'avancée des travaux, nos laboratoires de recherche et développement (R&D) sont tranquillement vidés de leurs contenus les plus précieux. En tout état de cause, ceux qui détiennent l'information détiennent tout.

Il est certain que l'intelligence économique recouvre les questions de recherche de l'information, mais il est aussi indubitable que ce concept regroupe, comme le précise Patrice de Gaudusson[2], en fait trois activités interdépendantes :

- la recherche de l'information,
- la protection et la sécurité du patrimoine
- et les actions d'influence ou de contre-influence.

Dès lors l'information devient l'enjeu de domination économique. Pour atteindre les objectifs inhérents à la quête de cette domination, les dérives vers l'espionnage industriel ne sont pas rares et pourraient s'apparenter à un véritable pillage économique de l'adversaire. Mais les informations « noires » ou « fermées », celles gardées jalousement secrètes, prennent une valeur inestimée pour le moment, conférant à ceux-là même qui les détiennent le statut de puissance.

[2] Revue d'Intelligence économique – décembre 2004

1 - Le traitement de l'information, enjeu de la guerre économique

1.1 - Le rôle stratégique de l'information

"La science économique enseigne que l'asymétrie d'informations - c'est-à-dire les situations où certains en savent plus que d'autres sur leur environnement - impose la conduite de comportements stratégiques. (…) Comme l'art de la guerre, se fondait naguère sur le renseignement, celui du commerce ne peut désormais se passer de savoir"[3]
L'information permet de mettre en évidence l'évolution du marché, en révélant les comportements des concurrents, leurs ambitions, les pays où ils commercialisent leurs produits ou services. Il faut donc surveiller la vitesse des évolutions de la science, de la technologie, des habitudes, afin de connaître les produits rentables financièrement ou les produits en déclin. La nécessité absolue d'innover, de ne pas se contenter de produire et de vivre sur ses acquis, a induit une prise de conscience croissante de l'intérêt de maîtriser parfaitement les informations concernant l'industrie et les services pour surveiller, se défendre, attaquer. Être au courant des évolutions dans son secteur d'activité est un impératif vital. Les données scientifiques, techniques, technologiques, technico-économiques évoluent sans cesse et impose de surveiller les tendances, de déceler les indices de changement, de deviner les synergies possibles, d'anticiper et d'être toujours prêt à innover. En résumé, l'information permet de mesurer le degré de liberté et de menace sur un marché pour une entreprise. La collecte d'informations dans ces domaines est donc au cœur des nouveaux défis de l'entreprise.

Selon H. Martre[4], « pour prendre des décisions économiques optimales, il faut comprendre la réalité dans laquelle elles s'appliquent. Comme dans l'impressionnisme, on se sert des éléments glanés ici et là pour brosser le tableau le plus proche possible de la réalité ». La connaissance de l'environnement est donc un facteur décisif dans la construction d'une prise de décision stratégique. Une étude menée auprès de chefs d'entreprise a permis d'effectuer un classement entre différents facteurs de compétitivité. Parmi les six facteurs arrivés en tête figurent : l'adaptation à la demande, la qualité de service, l'image de marque, le rapport qualité-prix, l'avance technologique et les méthodes de distribution. Or, ces six facteurs incorporent tous une proportion d'information considérable. S'adapter à la demande, améliorer la qualité du service suppose de bien connaître les besoins du client. L'image

[3] M. Christian Pierret, secrétaire d'État à l'industrie, IHEDN, 20 avril 2000

[4] Henri Martre : « intelligence économique et stratégie des entreprises » - Commissariat général du Plan – la documentation française - 1994

de marque résulte des efforts de communication intégrés dans la stratégie de l'entreprise. De même, l'avance technologique et la distribution nécessitent une recherche constante d'informations pertinentes. Ainsi, ce sont ces informations qui vont définir et encadrer le système de production, le système commercial, la recherche et le développement…Ainsi l'activité des concurrents oriente les axes de recherche. De même l'innovation se nourrit des travaux des laboratoires de recherche étrangers.

Dans un contexte économique concurrentiel et conflictuel, les entreprises se doivent d'être toujours en avance sur leurs adversaires. Aujourd'hui, c'est l'information, plus que tout autre facteur de production, qui procure un avantage compétitif. L'information économique permet de prévoir et donc d'anticiper les stratégies : développer de nouveaux produits, devenir plus performants, prendre des décisions, mieux vendre… Enjeu de survie et de développement des firmes, le renseignement économique stratégiquement utilisé au sein des Etats-nations peut devenir une arme de domination économique sur la scène mondiale.

1.2 - L'information, arme de domination économique

Les entreprises ou économies qui maîtrisent l'information sont aujourd'hui celles qui réussissent à s'imposer dans la compétition mondiale. Plus une économie est en mesure de collecter l'information, plus elle accroît sa puissance, et s'arme dans la guerre économique. Beaucoup plus qu'un enjeu de survie dans la compétition mondiale, l'information établit les rapports de forces entre nations.

Le Japon a été, incontestablement, la nation qui a su tirer le plus grand profit de l'information. A l'évidence, les Japonais l'utilisaient comme une arme nécessaire parmi d'autres pour gagner la guerre économique. Ainsi les auteurs du rapport « Japan 2000», (Christian HARBULOT. *La machine de guerre économique)* paru en 1991 aux États-Unis, décrivent le modèle japonais en ces termes : « La stratégie du Japon est axée sur la conquête, le contrôle et l'utilisation de la puissance. Toutefois, la puissance du Japon n'est pas construite sur une supériorité militaire mais essentiellement sur la connaissance et sur la technologie de l'information. L'acquisition de la connaissance a été et demeure toujours un fantastique atout de supériorité en faveur du Japon. » La recherche d'information fait partie intégrante de la tradition japonaise. Cette spécificité culturelle s'est révélée pendant plusieurs décennies un atout majeur dans la performance économique japonaise. Dès l'époque Meiji, la doctrine japonaise devient : « Nous irons chercher la connaissance dans le monde entier afin de renforcer les fondements du pouvoir impérial ». Ainsi, la méthode japonaise a longtemps défini un système d'ouverture vers « l'extérieur » dans le but d'enrichir «l'intérieur».

1.3 - Pouvoir et manipulation de l'information

Mais il faut prendre en compte le fait que cette information, arme de domination économique, peut amplement être manipulée.

Les techniques de manipulation de l'information, devenues des instruments offensifs et destructeurs face aux concurrents, sont nombreuses : sous-information, sur-information, effets de caisse de résonance ou encore désinformation. A l'origine ces méthodes ont été mises en pratique par les services secrets soviétiques. Aujourd'hui, les grandes entreprises, quelle que soit leur nationalité, les utilisent volontiers à des fins stratégiques.

- La sous-information consiste à filtrer et doser les informations qui sortent de l'entreprise ou du pays. Les renseignements alors disponibles sur le marché sont uniquement ceux que l'entreprise a bien voulu laisser s'échapper.
- La surinformation est, elle aussi, une tactique très efficace. Elle consiste à noyer ses concurrents sous la masse d'informations complexes, rendant leur traitement impossible. Ce danger menace aujourd'hui un grand nombre de pays, quand on sait que la quantité d'informations déversée sur le marché croît de 30% par an.
- La désinformation consiste à communiquer de fausses informations pour masquer les vraies et égarer ainsi l'adversaire vers une connaissance erronée de l'environnement. Cette tactique entraîne les concurrents à négliger des secteurs entiers pendant que l'entreprise responsable de la désinformation développe une stratégie agressive. Elle peut conduire ainsi à une élimination destructrice des adversaires. La désinformation est une pratique de plus en plus répandue et les exemples sont nombreux. Une société aéronautique américaine avait fait réaliser, il y a quelques années, une fausse étude de marché concernant le renouvellement des flottes aériennes. Elle s'est ensuite arrangée pour que cette étude soit acquise par des concurrents et les a donc lancés sur de fausses pistes.
- Sans être véritablement faussée, l'information peut également être influencée volontairement. C'est le cas de la technique dite des « caisses de résonance ». Une entreprise peut utiliser toutes sortes de moyens pour faire dériver l'information, qui circule sur son compte, de son objectivité. L'information « sous influence » est obtenue par des pratiques allant jusqu'à l'achat des faveurs de politiciens et autres membres administratifs. Une image de marque trop agressive peut ainsi être considérablement adoucie ; la méfiance des concurrents en sera d'autant plus affaiblie.

Bien maîtrisée et bien utilisée, l'information est une arme puissante au sein de la guerre économique. Elle permet de construire des stratégies offensives à condition d'être maîtrisée et efficacement gérée. Après l'effondrement du bloc communiste, la plupart des économies occidentales ont brutalement pris conscience de la nouvelle nature des conflits qui se jouaient sur la scène mondiale. Les économies qui avaient placé la chasse à l'information comme objectif majeur se sont imposées en tant que puissance économique. La guérilla de l'information dans laquelle se sont depuis peu lancés tous les pays

industrialisés s'organise selon des méthodes où les barrières de la déontologie sont parfois transgressées.

1.4 – Capter l'information par un système de veille

Le travail de captation de l'information sur de sources ouvertes s'établit essentiellement à partir de dispositifs de veille. Il convient ici de définir ces différents systèmes avant de s'attacher aux méthodes de recherche d'informations que l'on peut d'emblée qualifier de « noires ».

La veille en général peut se définir comme la mise en œuvre de dispositifs récurrents et méthodiques pour collecter, traiter, diffuser et suivre l'information utile. Il s'agit pour l'entreprise de se constituer une documentation grâce à l'utilisation d'instruments d'accès à des banques de données, à des systèmes de traitement automatisé de ces données et des outils d'analyse de l'information. Ces données entrent dans le système de veille et il en ressort des renseignements utiles à la prise de décisions stratégiques, notamment en matière de Recherche et Développement et de transferts de technologies. La veille est désormais multiforme, on en distingue plusieurs types :

- La veille technologique consiste en une surveillance des informations ayant trait aux recherches scientifiques, aux techniques de pointe ou aux nouveaux procédés de fabrication. Jakobiak[5] définissait la veille technologique comme étant « l'observation et l'analyse de l'environnement scientifique, technique et technologique et des impacts économiques présents et futurs, pour en déduire les menaces et les opportunités de développement".

- La veille concurrentielle s'intéresse aux concurrents actuels ou potentiels, aux nouveaux entrants sur le marché qui peuvent notamment apparaître avec des produits de substitution. Dans ce type de veille, on distingue également le *benchmarking* qui consiste à observer ce que les concurrents font de mieux dans le secteur.

- La veille commerciale consiste en une surveillance des informations relatives à l'environnement commercial de l'entreprise. Elle concerne les marchés, les appels d'offre, les clients et les fournisseurs. Au delà des études de marketing, il s'agit de s'intéresser à l'évolution des besoins des clients sur le long terme ou encore de retrouver rapidement une source d'approvisionnement en cas de défaillance d'un fournisseur.

- La veille juridique s'attache à suivre régulièrement et de manière rigoureuse la législation, la jurisprudence, les règlements nationaux, les directives européennes et les traités internationaux…

- La veille stratégique regroupe l'ensemble de ces différentes veilles ; elle constitue un processus d'aide à la décision qui vise à observer et à analyser l'ensemble des informations présentes dans l'environnement de l'entreprise en vue de définir ou d'infléchir la stratégie de l'entreprise.

---

[5] « Exemples commentés de veille technologique » - François Jakobiak - 1992

Parmi toutes ces veilles, celle technologique constitue un terrain juridique accidenté et il est souvent difficile de déterminer où finit la veille et où commence l'espionnage industriel. La délimitation de l'espionnage industriel aux seuls actes illégaux pose déjà un certain nombre de problèmes. En effet, les procédés utilisés sont très divers et tous ne peuvent pas tomber sous le coup de la loi, car comme nous le verrons, écouter une conversation ou engager un ancien employé d'un concurrent n'est en soi pas répréhensible.

Pour autant la veille ne doit pas être assimilée à de l'espionnage industriel car elle traite d'une part de l'information ouverte et recoupée mais se refuse à l'information volée; d'autre part elle repose sur une certaine déontologie, constituant un facteur décisif de reconnaissance de la discipline au milieu de l'entreprise. Il est vrai que la moralité et la déontologie constituent un second point de délimitation entre veille et espionnage industriel. Cependant, il ne faut pas croire que les chefs d'entreprise respectent toujours les principes éthiques fondamentaux. Et cela, pour deux raisons principales :

- c'est parfois une solution de facilité de transgresser la déontologie ; dans tout système, il existe des gens qui en toute bonne foi ne connaissent pas les codes de déontologie,
- d'un pays à l'autre, les lois et la déontologie peuvent varier ; il existe des différences légales mais aussi culturelles d'un pays à l'autre : les pratiques de pots de vin pour acheter des informations sont interdites dans les pays occidentaux, mais tolérées, voire obligatoire dans les pays orientaux.

1.5 - De l'intelligence économique à l'espionnage industriel

Les professionnels ont toujours su que le renseignement « ouvert » constitue, suivant les cas, de 80 à 95% du matériel nécessaire à la connaissance préalable à laquelle concourt l'espionnage. Villain[6] a répertorié les sources possibles d'information et conclu que 70% d'entre elles étaient disponibles sous formes d'informations ouvertes et 20% sous forme d'informations fermées mais légalement accessibles. Cette proportion s'est peu à peu modifiée. On peut considérer aujourd'hui qu'il est possible d'aller chercher près de 95% des informations nécessaires de façon « normale », notamment par un système de veille propre à chaque entreprise. Mais ces 90 à 95% ne servent pas à grand chose si les 5% à 10% de renseignement « fermé » manquent. Or, pour acquérir ce renseignement de sources fermées (documents internes d'entreprises, protocoles et résultats de recherche et développement, stratégies commerciales et moyens mis en place etc.) il faudra, presque obligatoirement, à un moment où l'autre, « franchir la ligne ».

---

[6] « L'entreprise aux aguets » - Villain - 1989

Certes, le fait de travailler sur « sources fermées » n'est pas, en soi, illégal. Aucune loi interdit à un individu ou à une société de prendre contact avec le détenteur de « renseignement fermé » et de le faire parler, pour autant que cela se passe ouvertement, sans corruption, sans contrainte et sans subterfuge. Mais même dans ce cas, le délit ne sera pas loin car, tôt ou tard, l'opérateur se retrouvera en possession d'informations commerciales ou industrielles qui ne lui sont pas destinées et pourra donc être accusé de recel de vol (ou de détournement) d'informations privilégiées. Dans la réalité, pour acquérir ce renseignement fermé, l'opérateur devra accumuler les délits, des « moins graves » (usurpation d'identité ou de fonction) aux plus lourds: organisation de surveillances physiques pouvant être assimilées à une intrusion dans la vie privée, corruption, chantage, vol, interception de courrier, écoutes illégales, intrusion informatique etc.

Ainsi dans bien des esprits, les notions de renseignement et d'espionnage sont confondues. En réalité, on peut collecter du renseignement de bien des manières sans jamais recourir à l'espionnage ni commettre d'acte illégal. Face au flou qui caractérise certaines de leurs pratiques, les professionnels de l'intelligence économique, autrement qualifié de renseignement économique, proclament volontiers leur souci de respecter la légalité et une certaine déontologie. Mais pour que cette affirmation ait un sens, il faudrait une définition claire de l'espionnage économique ou industriel, de ce que l'on peut faire et de ce que l'on ne doit pas faire. Or la barrière entre ce qui est permis et ce qui est interdit est loin d'être lisible en toutes circonstances. Les débats en cours parmi les professionnels révèlent les désaccords sur la nature des pratiques qui peuvent être considérées comme acceptables ou non[7].

Aux Etats-Unis, l'espionnage économique est défini comme « *the unlawful or clandestine targeting or acquisition of sensitive financial, trade, or economic policy information, proprietary economic information or critical technologies* ». C'est donc le caractère illégal ou clandestin de la recherche d'informations qui caractérise l'espionnage économique dans cette définition qui en exclut par conséquent le recueil d'informations disponibles dans le domaine public.
L'espionnage industriel est quant à lui défini comme « *the activity conducted by a foreign government or by a foreign company with the direct assistance of a foreign government against a private US company for the sole purpose of acquiring commercial secrets* ».

En fin de compte, l'espionnage viserait donc à capter de l'information « noire », c'est à dire celle qui est protégée et que l'on ne trouve pas dans le domaine public parce que le propriétaire a pris des mesures pour la garder secrète ou confidentielle. Il s'agit généralement d'informations relatives à des transactions commerciales, à des activités et ressources économiques, à des projets de recherche et

[7] Jérôme Dupré, *Renseignement et entreprise* – 2002.

développement, à des secrets de fabrication, à des inventions qui n'ont pas été déposées comme brevets, à des technologies de pointes, etc.

Selon Maurice Botbol[8], « il ne faut pas confondre intelligence économique et espionnage. L'intelligence économique se fait avec des moyens légaux en structurant sa recherche d'informations. L'espionnage économique se fait de manière totalement illégale. En fait, il y a une confusion entre les deux termes, parce que les techniques du renseignement sont en train de se diffuser au niveau des entreprises. Il y a beaucoup de personnes des services de renseignement, notamment aux Etats-Unis, qui ont été licenciées après la fin de la guerre froide et qui se sont retrouvés dans le domaine économique. »

La figure ci-dessous, se propose de bâtir une distinction entre intelligence économique et espionnage industriel autour de deux axes : l'axe légalité-moralité / illégalité immoralité et l'axe entreprise protégée / entreprise non protégée.

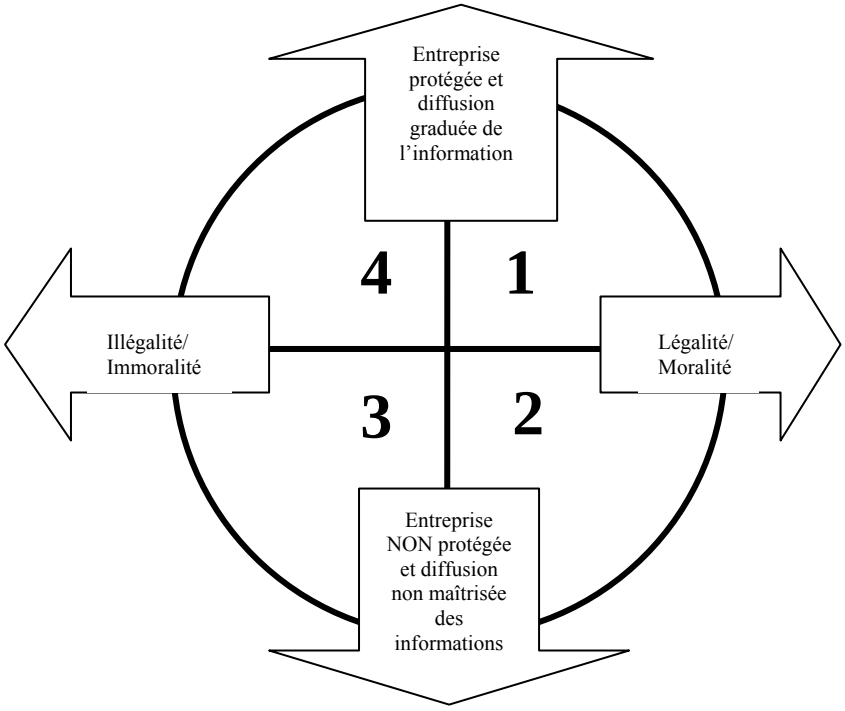

Figure 1 : Veille et espionnage : les limites

Le cadran 1 représente la veille "classique" active, c'est-à-dire la veille dans le cadre de la légalité et l'entreprise visée par le veilleur est protégée des attaques extérieures.

[8] M Botbol : directeur de publication de la lettre confidentielle 'Le Monde du Renseignement' et du site Intelligence Online

Le cadran 2 représente les cas où le veilleur repère les failles de l'entreprise cible. La veille est effectuée dans un cadre légal et moral, mais l'entreprise visée par le veilleur n'est pas protégée. Le veilleur risque d'être tenté de passer au cadran 3

Dans le cadran 3, le veilleur exploite toutes les failles de la cible. Les moyens employés se dirigent vers des actions illégales et immorales.

Enfin, dans le cadran 4, le veilleur fait de l'espionnage au sens strict. L'entreprise visée par le veilleur est protégée et le veilleur est définitivement tombé dans l'illégalité / immoralité.

Plus le veilleur progressera dans son étude de l'entreprise concurrente, plus les informations recherchées se feront fines et stratégiques, et plus il sera tenté d'utiliser des pratiques douteuses, proches de l'espionnage industriel.

La figure 2 ci-dessous définit l'existence de « zones grises ». Il est alors impossible de proposer une approche réaliste des phénomènes d'espionnage sans prendre en compte l'ensemble des «zones grises» qui gravitent autour de l'espionnage industriel au sens strict.

La fin (information recherchée)				
	Information noire (fermée, secrète)	Interdit	Interdit	Espionnage (au sens strict)
	information grise (semi ouverte)	Intelligence économique	Intelligence économique	Bêtise dangereuse
	information blanche (ouverte)	Intelligence économique	Bêtise dangereuse	Bêtise dangereuse
		ouverts	organisés et déontologiques	illégaux
			Les moyens utilisés	

Figure 2 : les zones grises de la recherche d'informations[9]

Dans les systèmes d'intelligence économique, même si ceux-ci reposent au départ sur une éthique précise, l'espionnage apparaît comme un moyen de rechercher chez ses concurrents une information déterminante pour l'économie nationale. Souvent, il existe des liens très forts entre les organismes chargés de l'intelligence économique et les services secrets officiels, quand ceux-ci ne sont pas confondus. L'espionnage industriel s'intègre dans une démarche progressive. La recherche d'informations débute par la mise en place d'un système de veille (zone blanche), puis dérive progressivement vers l'espionnage industriel. Mais très vite il apparaît à quel point il est difficile de délimiter les différents niveaux de gravité des pratiques « douteuses ».

[9] Source : B. Martinet, Y-M Marti. L'intelligence économique. Paris : les Editions d'Organisation, 1995.

Il apparaît donc impossible de fixer strictement une limite juridique ou déontologique à l'espionnage industriel. L'espionnage est un bon complément de la veille, c'est pourquoi les entreprises n'hésitent plus à y avoir recours.

2 - L'espionnage industriel ou l'organisation du pillage économique

L'espionnage industriel est, comme nous venons de le voir, une pratique qui prête à confusion avec les systèmes de veille et d'intelligence économique. Délimiter trop strictement ce concept peut s'avérer dangereux ; construire une définition trop stricte reviendrait à nier un grand nombre de réalités de l'espionnage industriel. Espionner ses concurrents représente la démarche aboutie de la recherche d'information. Ces pratiques sont de plus en plus répandues aujourd'hui et sont la source de nombreux préjudices économiques.

En réalité, les limites entre les concepts de veille technologique, intelligence économique et espionnage industriel sont souvent floues ; les tentations sont grandes de transgresser les règles d'éthique. L'espionnage industriel est souvent décrit comme un dérivé malsain de la veille technologique, le « cancer » de l'intelligence économique. Il s'agit de l'ensemble des pratiques à travers lesquelles les informations sont obtenues par des moyens répréhensibles (corruption, piratage, vols de documents…). Cette pratique se trouve très proche des méthodes de renseignement militaire et sort des limites de la morale et de la légalité.

2.1 – Les fondements de l'espionnage industriel

Face à la situation de perpétuelle concurrence au niveau mondial, de mondialisation des échanges, c'est-à-dire de guerre économique, l'information a acquis une valeur croissante. Dès lors la veille semble souffrir de certaines insuffisances face aux attentes de plus en plus précises des chefs d'entreprises. L'intérêt est grand et d'une rentabilité certaine d'aller dérober les avantages d'autres entreprises par le biais de l'espionnage. Dans un monde dominé par la technologie, les secrets commerciaux, formule, conception, plan de marketing sont la nouvelle monnaie d'échange sur le marché. L'espionnage industriel est une méthode efficace pour obtenir une information de bonne qualité et non détournée, puisqu'elle est récupérée au sein de l'entreprise elle-même.

La motivation première des agents économiques qui s'adonnent à l'espionnage est d'abord le gain de temps et surtout d'argent que cette pratique procure. Dans la nouvelle donne économique mondiale, il faut aller le plus vite possible et ceci aux moindres frais. Or, la recherche et le développement, de plus en plus sollicités face à la forte demande d'innovations, est un processus très lent, dont les coûts se sont multipliés ces dernières années. Quand on sait qu'il faut, en moyenne, douze ans de travail et 231 millions de dollars aujourd'hui pour mettre un nouveau médicament sur le marché américain, on comprend que les milieux pharmaceutiques soient les proies d'un espionnage intensif. Ainsi, le

renseignement, obtenu par des moyens illégaux, peut faire épargner des années et des milliers d'euros à des firmes, si elles devaient acquérir certains secrets par des voies légales.
Opter pour l'espionnage est, de plus, facilité par l'accessibilité des moyens et des techniques. Mettre en place un système de veille nécessite un investissement long et coûteux. L'entreprise doit se créer un fonds documentaire, embaucher du personnel… Faire appel à des cabinets de conseil spécialisés en veille coûte en moyenne 4500 euros par mois. Nombreuses sont donc les entreprises qui préfèrent utiliser directement des techniques d'espionnage.

Contrairement à la veille, c'est parce qu'il est de plus en plus facile de se doter des techniques, que l'espionnage gagne du terrain dans les entreprises. Avec quelques milliers de dollars et un peu de savoir-faire, il est désormais possible de fabriquer un attirail électronique qui permet d'entendre une conversation, d'intercepter des appels, de savoir ce qui se passe sur un ordinateur à trente mètres… De la même manière on peut se demander pourquoi dépenser dix ans de travail et un milliard de dollars en recherche et développement quand il est possible de corrompre un ingénieur de l'entreprise concurrente pour un million de dollars et obtenir le même résultat, si ce n'est mieux.

2.2 – Moyens et procédés de l'espionnage industriel

Que ce soit en Asie ou en Occident, les actes délictueux d'espionnage sont en train de devenir un excellent raccourci pour l'emporter sur la concurrence. Les méthodes utilisées pour rassembler les renseignements économiques sont à la fois légales, illégales, traditionnelles et de plus en plus novatrices. Nous n'avons pas l'ambition de faire une liste exhaustive de toutes les méthodes employées ; elles sont trop nombreuses, d'autant plus que le domaine évolue constamment.
Retenons tout d'abord que la démarche des espions est progressive :
- dans un premier temps, les agents de renseignement s'attaquent aux informations disponibles et ouvertes. Ces méthodes s'apparentent encore à la veille, mais se révèlent parfois offensives ;
- dans un second temps, les espions vont chercher à provoquer la sortie d'information en dehors de l'entreprise. Ces méthodes ne tombent pas toutes sous le coup de la loi mais transgressent la plupart du temps les principes de la déontologie ;
- enfin, pour obtenir une information encore plus précise, il peut s'avérer nécessaire de pénétrer dans plusieurs services fermés de l'entreprise. Pour cela, les espions ont souvent recours à des moyens illégaux comme le piratage informatique, les écoutes téléphoniques, la corruption du personnel interne…Ces intrusions peuvent également se faire ouvertement par l'intermédiaire de collaborateurs de recherche ou autres stagiaires.

a - Le recueil de l''information « grise »

L'information grise est celle qui, n'étant pas publiée, s'obtient de manière informelle, auprès de personnes appartenant à l'entreprise elle-même ou du monde extérieur (clients, fournisseurs, sous-traitants, experts, etc.). Ces informations, pas nécessairement confidentielles, peuvent être riches d'une grande valeur ajoutée et contenir des « signaux faibles » annonceurs de menaces ou d'opportunités pour l'organisation. En matière de renseignement, les oreilles sont partout. Les concurrents n'hésitent pas à placer des agents dans des lieux fréquentés par les employés de l'entreprise. Écouter une conversation entre deux chercheurs peut se révéler très instructif. De nombreux contrats ont été perdus par des bavardages dans le TGV, sur des lignes aériennes ou des restaurants d'affaires.

La littérature relative à l'intelligence économique ou aux services de renseignement livre de nombreuses manières de recueillir ce type d'information, des plus classiques aux plus sophistiquées, mais pas nécessairement déloyales ou illicites. En voici ici quelque aperçu.

- Les réseaux d'informateurs des entreprises.

Certaines entreprises mettent sur pied de véritables réseaux de correspondants spécialisés chargés d'observer et de recueillir des renseignements de nature informelle, non structurée. Ils utilisent, pour transmettre leurs informations aux analystes, des formulaires standardisés aussi appelés "capteurs d'informations". Ce sont soit des "voyageurs" de l'entreprise, soit des représentants, qui par leurs contacts privilégiés avec les fournisseurs, les sous-traitants, les clients, peuvent obtenir de l'information fraîche sur les besoins, les projets, les évolutions des concurrents.

- La fréquentation des expositions, des colloques, congrès, foires et salons.

Ces rassemblements d'experts constituent une source considérable d'information pour les professionnels de l'intelligence économique, ... et pour les espions. Les comptes rendus en sont systématiquement étudiés. Les prospectus intéressants sont récoltés pour être passés au scanner et introduits dans des banques de données. Des échantillons sont analysés, des pièces sont photographiées - parfois clandestinement -, des spécimens sont acquis (ou dérobés) pour être décortiqués.

- Les visites d'entreprise.

Les entreprises se montrent le plus souvent accueillantes envers les visiteurs. Ainsi, même s'il faut reconnaitre que ces intrusions représentent un risque significatif, dans la plupart des cas, les visiteurs peuvent avoir accès à tous les services de l'entreprise. Ces visiteurs qui prennent des photos, font des croquis ou ramassent sur le sol des poussières de matériaux composites appartiennent aussi à l'armée des agents du renseignement. Un scientifique très compétent peut se faire une idée précise des axes de recherches et de leur état d'avancement rien qu'en jetant un coup d'œil sur les équipements d'un laboratoire. Ces visites permettent de repérer les systèmes de management, l'aménagement des usines…Le risque est donc bien moins celui d'une expédition nocturne que celui d'une visite courtoise et ouverte.

b - Le recueil de l'information « noire »

Les méthodes les plus classiques et brutales sont bien sûr le vol de documents, la fouille des poubelles, la subornation de personnes, la corruption, le chantage, les menaces, etc. Des techniques de manipulation peuvent également être mises en œuvre, sans parler des technologies nouvelles. On peut aussi citer les méthodes suivantes.

- La surveillance des scientifiques en voyage à l'étranger.

Un rapport présenté le 25 juin 2000 par le *"General accounting Office"* (GAO) au Congrès des Etats-Unis a recensé 75 tentatives récentes d'espionnage à l'étranger sur des savants nucléaires américains. Ce rapport expose des cas de mises sous écoute dans des hôtels, de fouilles d'effets personnels ou bien encore d'offres de services de prostituées.

- Les chercheurs universitaires en stage à l'étranger.

Les laboratoires universitaires peuvent aussi être la cible de services de renseignement. La technique consiste à y envoyer des étudiants boursiers ou des chercheurs stagiaires pour y recueillir des informations importantes d'ordre scientifique. Le séjour terminé, l'étudiant chercheur sera soigneusement "débriefé" de ses connaissances techniques et scientifiques fraîchement acquises. Le monde académique se montre en général assez ouvert à la diffusion du savoir et à la coopération internationale, d'où la facilité pour n'importe quel chercheur de recueillir des informations sans même les avoir demandées. La France accueille chaque année entre 60 000 et 100 000 stagiaires étrangers dans ses entreprises, ses laboratoires, ses centres de recherche. Certains chefs d'entreprise n'hésitent pas à utiliser l'expression de « péril jeune[10] ». La DST a établi que la majorité des stagiaires, surtout en provenance d'Asie et d'Europe de l'Est ont reçu une mission de renseignement.

L'affaire de la jeune chinoise Li Li Whuang, stagiaire chez l'équipementier automobile Valeo, soupçonnée d'espionnage industriel par la justice française, est loin d'être unique en son genre.

- Les faux appels d'offres.

Un Etat fait savoir par des appels d'offres qu'il désire se rendre acquéreur d'une licence d'exploitation ou d'une usine livrée clé sur porte. Aussitôt sollicitées, les grandes sociétés réagissent en dépêchant sur place leurs ingénieurs commerciaux. Les tractations traînant en longueur, les sociétés en lice fournissent de plus en plus d'informations sur leur offre sans y voir malice, espérant obtenir le marché. Elles livrent ainsi des renseignements qu'attendait le pays demandeur. Une firme privée peut aussi agir de la sorte en se présentant, via un cabinet d'investigation, comme client potentiel.

- Les fausses annonces de recrutement.

Les cabinets de recrutement peuvent aussi servir à la collecte de renseignements d'ordre économique. La méthode consiste à publier une annonce alléchante capable de retenir l'attention de cadres ou de

---

[10] Germain CHAMBOST. « Après la guerre froide, la guerre économique », *Science et Vie,* n°921, juin 1994.

chercheurs d'une entreprise cible. Les personnes intéressées par une meilleure proposition salariale, des conditions de recherche améliorées et divers avantages (appartement et voiture de fonction, indemnités diverses, etc.) expédient leur C.V. Celles-ci sont convoquées pour un entretien au cours duquel elles sont longuement interrogées sur leur qualification, leurs travaux antérieurs et actuels. Désireuses d'obtenir le poste, elles sont susceptibles de chercher à se faire valoir en livrant des informations confidentielles qui ne manqueront pas d'intéresser la société concurrente ou l'Etat caché derrière le bureau de recrutement. Ainsi sans embaucher personne, le recruteur connaît tout de la stratégie et des axes de recherche de ses concurrents.

- L'interception des communications (COMINT[11]).

L'existence d'un réseau global d'interception des communications baptisé "ECHELON" mis en place par les Etats-Unis et par les autres Etats membres de l'alliance UKUSA[12] a été médiatisée dés septembre 1998 par une série de rapports destinés au Parlement européen. Ce système orienté à l'origine vers le bloc de l'Est, aurait été détourné de sa finalité militaire initiale bien avant l'effondrement des régimes communistes. Le chapitre 5 intitulé "*Comint and economic intelligence*" contient quelques passages intéressants qui indiquent notamment : *"Comint involving the covert interception of foreign communications has been practiced by almost every advanced nation since international telecommunication became available. Comint is a large-scale industrial activity providing consumers with intelligence on diplomatic, economic and scientific developments.(...) Since the 1960s, following the growth of world trade, the collection of economic intelligence and information about scientific and technical developments has been an increasingly important aspect of Comint"*.

La législation des pays membres de l'alliance UKUSA autorise en effet leurs agences de renseignement ainsi que certains ministères à programmer la recherche de renseignements d'ordre économique ou commercial et à en recevoir par le recours au Comint.

L'organisation UKUSA et son système d'espionnage planétaire « Échelon » est l'exemple type d'action d'intelligence stratégique relevant de la violence légale dans les pays l'ayant institué mais devenant totalement criminel dès l'instant où ce système s'étend à d'autres pays, même officiellement alliés. On se souviendra du voyage officiel en Arabie Saoudite du premier ministre français Édouard Balladur fin 1994 dans le cadre duquel était prévue la signature d'un très important contrat de fournitures d'équipements aéronautiques militaires qui n'eut finalement pas lieu car quelques jours auparavant une firme américaine envoya une offre légèrement meilleure en tous points qu'elle avait pu établir, on le sait aujourd'hui, grâce aux renseignements de dernière heure obtenus par le système

---

[11] Le concept Comint (communication intelligence) est défini comme étant la collecte de renseignements effectuée par la surveillance des télécommunications et l'interception de leur contenu.

12 Il s'agirait d'une entente secrète de 1947 organisant la coopération entre les Etats-Unis, le Royaume Uni, le Canada, l'Australie et la Nouvelle Zélande en matière de renseignements.

Échelon. Outre l'humiliation subie, ce fut surtout une grosse perte pour les industriels d'un pays qui n'a pas la chance d'appartenir à UKUSA…

En effet, à ce jour, les données collectées sur les cinq continents par le système Echelon sont acheminées aux Etats-Unis où elles sont traitées par la NSA (National Security Agency). Si celle-ci affirme que les informations ainsi obtenues concernent prioritairement le grand banditisme, la lutte anti-terroriste et la prolifération des armements, on a du mal à croire que le système n'est pas également intensivement exploité dans les programmes d'espionnage économique et autre veille concurrentielle.

- La prise de participation dans une société et les accords de coopération entre firmes.

Certaines entreprises engagées dans la veille technologique dispose de fonds d'investissement afin de prendre des participations dans des sociétés de haute technologie. Une personne "neutre", agissant pour le compte d'une compagnie (ou d'un Etat) qui désire rester dans l'ombre, procède - grâce à des sociétés-écrans et des relais - à la prise de participation dans la société cible, par exemple lorsque celle-ci est fournisseur dans un secteur de pointe. Cela permet d'avoir accès à des informations d'ordre technologique, éventuellement à du matériel classifié ou de vendre du matériel soumis à embargo.

Le développement des accords de coopération entre firmes constitue une autre vulnérabilité. Les entreprises sont amenées à travailler en coopération de plus en plus étroite avec beaucoup de partenaires industriels et à les associer aux phases d'études et de mise au point. Ces politiques d'accords de joint-ventures, recherches groupées, co-production et autres multiplient les risques de fuite. Les personnels des deux entreprises sont amenés à travailler ensemble et donc à fournir un accès potentiel aux informations scientifiques et techniques. L'accès peut être intentionnel ou non, légal ou illégal.

Le rachat pur et simple ou la prise de contrôle de la cible pourrait constituer l'arme absolue pour obtenir des informations secrètes détenues par une entreprise ou un laboratoire. La multitude de PME qui font de la sous-traitance dans les secteurs de pointe sont des objectifs très vulnérables. En utilisant toute une série de sociétés-écrans, on peut s'assurer tous les pouvoirs chez les sous-traitants de THALES, d'EADS et, sans être inquiétés, récupérer ainsi tous les secrets jusqu'alors les mieux gardés.

Pour obtenir une information vitale, les agents du renseignement ne reculent devant rien. Les dérapages sont plus ou moins graves, mais dans tous les cas l'entreprise victime doit faire face à des pertes toujours importantes.

Dans la guerre économique actuelle, l'organisation bipolaire de l'espionnage industriel, héritage de l'affrontement des deux blocs, a volé en éclats. Les acteurs se sont multipliés, de nouveaux ennemis ont émergé et les services officiels ont été contraints de se reconvertir. Les secteurs visés ne peuvent plus être aussi clairement identifiés. L'espionnage industriel actuel repose donc sur une structure éclatée où la nature des acteurs et de leurs objectifs s'élargit continuellement.

2.3 - Les acteurs et les cibles

a- Les acteurs

L'espionnage industriel peut être pratiqué :

- soit par les États et leurs services secrets de renseignement : c'est l'espionnage d'État ou public. Le centre européen pour le renseignement stratégique et la sécurité (ESISC), basé à Bruxelles, a révélé qu'un véritable réseau d'espionnage économique chinois, dont la base se trouverait au sein de l'université de Louvain, essaimerait dans toute l'Europe du Nord. D'après Jacques Baud[13], « La Chine est considérée comme l'un des pays les plus agressifs en matière d'intelligence économique ».
- soit par les entreprises elles-mêmes contre d'autres entreprises nationales ou étrangères : c'est l'espionnage privé.

- L'espionnage public :

L'espionnage public est au service des pouvoirs d'une nation ; il est initié par les services secrets nationaux et vise toutes les informations qui peuvent se révéler utiles à l'industrie et à l'économie nationale. C'est l'un des moyens utilisés par de nombreux pays pour améliorer ou conforter leur position politique, militaire, économique, scientifique ou technologique face à leurs adversaires.

Rares sont les gouvernements qui n'ont pas créé des services de renseignements. Après la fin de la Guerre Froide, la plupart de ces services se sont reconvertis dans l'espionnage industriel; ces organismes étatiques ont une puissance considérable en la matière. On estime aujourd'hui à 1,5 millions de personnes les effectifs mondiaux de l'espionnage et du contre-espionnage, tous camps confondus. Un budget annuel de l'ordre de 20 milliards d'euros correspondrait à l'ensemble de ces activités.

Cependant, l'avis des différents services de renseignements nationaux diffère, quant à savoir quelle est la position à adopter en matière d'espionnage industriel. Pour les Américains, il est hors de question que la CIA ou la NSA (National Security Agency) redistribuent les informations qu'elles recueillent. A qui faudrait-il remettre de telles informations ? Qui en définirait les axes de recherche ? Le gouvernement ne fausserait-il pas ainsi les lois du marché? Cependant une structure de coordination qui réunit les dirigeants de dix-neuf administrations gouvernementales a été constituée et agit comme « un cabinet de crise » : l'*Open Source Center*[14]. Ce dernier a pour but de jeter tout son poids dans la bataille dès lors qu'un groupe industriel cherche à enlever un marché.

---

[13] Jacques Baud, auteur de l'ouvrage de référence l'Encyclopédie du renseignement et des services secrets

[14] Open Source Center : agence de renseignement, créée en 2005, consacrée aux sources ouvertes, chargée de collecter et d'analyser les informations.

– L’espionnage privé

Si le renseignement et l’espionnage étaient autrefois l’apanage exclusif des monarques et gouvernements, ils tiennent désormais une place importante dans le monde des affaires internationales, sous le nom d’espionnage privé. On peut considérer que l’espionnage industriel dans le monde des affaires fait désormais partie de la vie quotidienne des entreprises. Si les États-Unis se défendent de pratiquer l’espionnage industriel, ce n’est pas le cas de ses entreprises. Par nécessité et faute d’être aidées par leur gouvernement, les firmes américaines sont leaders du marché de l’espionnage privé.

Une entreprise qui désire espionner ses concurrents possède plusieurs solutions : elle peut engager d’anciens cadres de services secrets nationaux, mettre en place sa propre cellule de renseignement ou encore faire appel à des sociétés privées spécialisées. Ces privés interviennent sur commande à des tarifs motivants. De grosses sociétés, partout dans le monde, particulièrement en Occident et en Asie engagent désormais des agents expérimentés pour se procurer des renseignements sur leurs concurrents et sur les autres pays. Les multinationales du monde entier s’arrachent désormais d’anciens agents d’Europe de l’Est, réputés comme les meilleurs. Des sociétés comme Eastman Kodak, American Telephone & Telegraph, MCI Communication, Xerox, McDonnel Douglas, Ford…ont toutes engagé d’anciens agents spéciaux au cours des dernières années. De plus, un nombre grandissant de firmes américaines se sont dotées de véritables organes de renseignements.

L’essor de l’espionnage, au sein du monde des affaires, se caractérise par l’apparition d’un nombre croissant de sociétés privées qui rivalisent avec les services étatiques. Elles se sont multipliées sous des apparences diverses mais légales : sociétés de consultant, d’audit, cabinets de conseil en « sécurité et gestion de crises », agences de détectives ; cependant, les moyens qu’elles emploient pour se procurer des informations sont loin d’être conformes aux législations en vigueur. Aux États-Unis, nombre d’agents de la CIA ont créé leurs propres sociétés indépendantes telles que Kroll.

Les agents spécialisés dans le pillage du renseignement économique se sont donc considérablement multipliés, qu’ils soient commandités par les services étatiques ou bien par les sociétés privées. Dans le même temps, la nature des informations visées s’est, elle aussi, profondément modifiée. La gamme des secrets volés s’est largement étendue.

b - Les cibles

Il convient à présent de nous intéresser aux objectifs des espions, c'est-à-dire les informations-cibles. Quelles sont les renseignements les plus recherchés ? Quels sont les secteurs sensibles et les entreprises visées ? Quels sont les pays placés dans la ligne de mire des espions ?

– Les informations-cibles au sein de l'entreprise

Dans les entreprises, les risques sont partout où il existe un profit. Ce sont, évidemment, les procédés, les techniques et les méthodes de production d'un nouveau produit qui font le plus l'objet de convoitises. Les échantillons sont dérobés afin d'être analysés puis copiés. Cependant, dans le domaine commercial, l'espionnage industriel fait de plus en plus de ravages. Prendre connaissance des stratégies de développement de ses concurrents (participations, fusions, acquisitions, joint-ventures) avant même qu'ils ne les mettent en œuvre permet souvent de gagner d'importants marchés. On ne compte plus chaque année le nombre de vols, de fuites, de détournements de ce qui constitue le cœur de la logistique commerciale de l'entreprise : le fichier.

Selon une étude réalisée en mai 1988 par l'Université de l'Illinois, à Chicago, intitulée «Etude sur le vol de secrets commerciaux dans les industries de haute technologie», les cibles les plus fréquentes des espions, dans les 150 entreprises américaines interrogées, étaient les informations et données concernant la recherche et la technologie (86%), bien plus convoitées que les fichiers de la clientèle (28,8%), les secrets d'ordres financiers (21,2%) et les projets de programmes (24,2%). Recherche & Développement et Laboratoire sont les secteurs les plus visés, devant la Direction Générale, le Secrétariat Général, le service financier, viennent ensuite les secteurs marketing et commerciaux. Plans et budgets sont également très convoités tout comme les projets, soumissions et dossiers d'études. Cependant, les déchets, ordures et autres papiers ne sont pas non plus à négliger.

– Les entreprises-cibles

La chasse au renseignement se dirige en priorité vers les usines des grands groupes et les centres de recherche scientifique mais aussi vers les administrations. En réalité, aujourd'hui, ce n'est plus seulement l'industrie avec ses secrets de fabrication et son savoir-faire qui est visée, ce sont aussi les banques, les sociétés financières, la bourse, les agents de change…

Les cibles secondaires font l'objet de beaucoup d'inquiétudes : sous-traitants ou prestataires de service constituent des professions particulièrement travaillées par les chasseurs d'informations. Parmi ces nouvelles victimes se trouvent : les agences de publicité - où les campagnes pour les nouveaux produits se concoctent des mois à l'avance -, les imprimeries - qui préparent toute la documentation technique et commerciale -, les fabricants de moules et modèles, les maquettistes, photographes, consultants… N'importe quelle entreprise peut être victime de telles exactions. Tous les domaines de l'économie sont désormais touchés.

Classiquement, les secteurs les plus visés sont les secteurs de pointe dans lesquels la recherche fondamentale fait l'objet de gros investissements, et les secteurs de forte concurrence commerciale. La liste des secteurs sensibles de l'économie s'est, de plus, considérablement allongée. Il y avait l'armement, le nucléaire, l'espace, l'électronique ; maintenant les opérations d'espionnage industriel se multiplient dans la chimie, l'horlogerie, l'agro-alimentaire, la mécanique, le textile, le design, la mode…

– Les pays et organisations-cibles

Tous les pays ne sont pas touchés de manière identique par l'espionnage industriel.

La France serait aujourd'hui l'un des pays les plus pillés ; ses laboratoires et entreprises se vident de leurs secrets industriels ; cependant, de nombreuses brèches ont déjà été rebouchées grâce à une prise de conscience accrue des entreprises.

Les États-Unis par leur puissance technologique et commerciale, sont une cible privilégiée pour tous les services de renseignements de la planète. La CIA a établi la « *shopping list* » des secrets de haute technologie convoités par l'intelligence française. Cette liste mentionne dans leur ordre de priorité pour les espions français : l'informatique, l'électronique, les télécommunications, l'aéronautique et l'armement, le nucléaire, la chimie, l'espace et les biens de consommation. Durant l'année 1996, les États-Unis ont recensé douze pays impliqués dans des affaires d'espionnage à l'encontre d'entreprises américaines; à la même époque vingt-six pays supplémentaires sont suspectés et font l'objet d'investigations. Le Canada, l'Australie recensent également chaque année un nombre important d'actes d'espionnage industriel. Les milieux d'affaires allemands sont, eux aussi, inquiets devant la fuite de leurs secrets. Beaucoup de chefs d'entreprise ont déjà tiré la sonnette d'alarme auprès du gouvernement et sont allés jusqu'à qualifier le marché allemand de « véritable supermarché en libre-service ». En Allemagne, parmi les cibles privilégiées des espions, se trouvent, en premier lieu, l'industrie chimique et pharmaceutique, la branche aéronautique et spatiale, les constructeurs automobiles et l'électronique.

c- Exemple d'une affaire récente : Messier - Dowty

Les méthodes décrites précédemment peuvent parfois sembler extrêmes. Cependant, en quelques années, les affaires d'espionnage industriel ont fait de nombreuses fois l'actualité. Armement, pharmacie, transport, agroalimentaire, enseignement supérieur... Aucun secteur économique n'est épargné. Plus personne n'est à l'abri. Même des sociétés sensibles aux activités duales (militaires et civiles) ne semblent pas suffisamment protégées contre ces menaces. L'exemple de l'affaire Messier – Dowty illustre la tournure que peut prendre l'espionnage industriel.

Située à Bidos (Pyrénées-Atlantiques), Messier-Dowty, qui domine le marché mondial des trains d'atterrissage, travaille pour l'aviation civile et militaire. Or, le 7 novembre 2000, deux pièces du train d'atterrissage du Rafale Marine disparaissent. Ces éléments sont classés « stratégiques », ce qui oblige la Direction de la surveillance du territoire (DST) à enquêter. La direction de l'usine évoque alors une erreur d'aiguillage entre ses différents fournisseurs et prestataires. La thèse de l'espionnage économique demeure néanmoins, car quelques mois après la disparition de Bidos, des archives de Messier-Dowty contenant quelques secrets de fabrication ont été dérobées. De plus, en juillet 2003,

quatorze ordinateurs appartenant aux équipes d'ingénieurs qui travaillent sur le futur avion de transport militaire A400M ont été subtilisés. La thèse du vol par un pays allié circule toujours. Cette imputation est restée au stade de la présomption, car aucune preuve formelle n'accuse ces sociétés étrangères. Les pistes russe et américaine ont été sérieusement évoquées, mais ces hypothèses trop explosives ont été rapidement écartées, par peur de déclencher une cascade d'ennuis diplomatiques.

L'affaire Messier-Dowty témoigne des relations tendues entre les Etats via leurs bras armés économiques, les multinationales. Si les Etats peuvent être des alliés politiques, ils n'en demeurent pas moins de rudes adversaires économiques.

2.4 - Des espions non inquiétés

Personne ne peut aujourd'hui ignorer la réalité de l'espionnage industriel. Les conséquences en sont désastreuses pour les entreprises mais aussi pour l'économie du pays tout entier. Pour les grandes sociétés françaises, le préjudice général de l'espionnage industriel s'élèverait à 1,5 milliards d'euros par an[15].

Malgré ces chiffres accablants, il semble que l'espionnage reste encore dans l'ombre. Les gouvernements hésitent à dénoncer des actes d'espionnage sur le devant de la scène car ceux-ci touchent trop à la sécurité nationale. Pour les entreprises, les conséquences, qu'elles soient commerciales ou financières, sont toujours très importantes et peuvent aller jusqu'à nuire à la survie de l'entreprise. Cependant, rares sont les entreprises qui osent aujourd'hui se lancer dans des poursuites judiciaires.

L'espionnage industriel est une arme silencieuse. Personne dans les milieux politiques ou économiques ne semble vraiment disposé à porter les espions en accusation. Entre firmes, les dénonciations existent, certes ; mais, pour une plainte déposée, combien d'entreprises auront préféré jeter l'éponge ? De plus, la plainte aura-t-elle une chance d'atteindre son but ?

Dans la plupart des pays, les pouvoirs politiques ne semblent pas pleinement disposés à sanctionner l'espionnage industriel à hauteur des conséquences qu'il entraîne. La loi du silence s'impose d'elle-même. Les gouvernements se heurtent en effet à l'obstacle majeur que représente le risque de tensions diplomatiques. Les milieux d'affaires sont, eux aussi, très réticents. Faire éclater une affaire au grand jour implique d'en accepter les risques.

---

[15] Source La Tribune 29/11/2000

- les risques de tensions diplomatiques

Les milieux politiques hésitent à aborder le sujet car il est source de tensions diplomatiques. L'existence de l'espionnage entre «amis » que se livrent la France, Israël, l'Allemagne, le Japon et les États-Unis est désormais un fait connu de tous. Cependant, les dénonciations grand public de tels actes sont toujours restées des faits rarissimes. La coopération entre les différents pays est aujourd'hui si forte que peu osent prendre le risque d'enclencher des problèmes diplomatiques.

En février 1995, l'affaire de l'espionnage américain en France a fait grand bruit. Le gouvernement français souhaitait le départ du territoire français de cinq ressortissants américains, dont quatre bénéficiaient de l'immunité diplomatique, pour faits d'espionnage économique. Les affrontements diplomatiques furent de taille, d'autant plus que la France avait révélé cette affaire dans un contexte électoral aux États-Unis. Les deux parties tentèrent cependant rapidement d'éviter les surenchères diplomatiques. En fin de compte, le conflit fut traité à l'amiable ; les représentants américains gardèrent leurs postes à Paris et ne furent pas inquiétés outre mesure. En effet, le moment d'une crise diplomatique était d'autant plus mal choisi que la coopération entre les deux pays était essentielle pour empêcher une reprise de la guerre en ex-Yougoslavie. D'autre part, Français et Américains étaient en passe de renégocier un pacte de sécurité transatlantique.

- les craintes dans le monde des affaires

Les milieux économiques, eux aussi, restent muets devant l'espionnage industriel. Beaucoup préfèrent garder le silence pour ne pas nuire à leur image ou par peur de devoir détailler les preuves. Si des affaires éclatent, la justice n'est utilisée qu'en dernier recours. Les sanctions imposées aux victimes couvrent rarement le préjudice subi par la victime. Les entreprises sont rares à avouer avoir été victimes d'espionnage industriel. Cela revient, en effet, pour un chef d'entreprise à avouer ses faiblesses et donner ainsi prise aux critiques. Aucune entreprise n'avouera jamais avoir commis des erreurs de management en matière de sécurité.

De plus, lors du procès, l'entreprise victime se doit de fournir une preuve du vol et donc de dévoiler la nature des documents dérobés. L'information confidentielle devra donc être médiatisée devant le tribunal. C'est l'une des raisons les plus fréquemment avancée pour résoudre les victimes au silence, car la victime d'espionnage industriel serait amenée à rendre publique l'information dont elle se plaint d'avoir été volé.

2.5 - La protection du patrimoine de l'entreprise

a - Les armes de la propriété industrielle

L'entreprise, aux vues des menaces qui pèsent sur elle, doit être consciente qu'elle a le devoir de protéger sa technologie, son savoir-faire, ses innovations, ses écrits, ses hommes, c'est-à-dire tout ce qui constitue sa richesse, son patrimoine intellectuel et industriel. Toute fuite d'informations relative à ce patrimoine peut être utilisée par la concurrence et se traduit par une perte d'activité ou de profit pour l'entreprise et par conséquent pour la nation.

Les difficultés en matière de sécurité sont nombreuses. L'entreprise doit savoir protéger l'ensemble des informations ; celles émises par l'entreprise elle-même et qui concernent les études, la mise au point de produit, de savoir-faire, les gammes de fabrication, de montage, de contrôle, l'élaboration des stratégies commerciales, financières, mais aussi celles acquises à l'extérieur et qui font également partie de sa richesse.

Le problème est donc bien de maîtriser le flux d'informations sortant de l'entreprise et faire en sorte que seules les informations strictement indispensables aux relations avec l'extérieur sortent effectivement de l'entreprise, c'est-à-dire celles qui permettront aux agents commerciaux de vanter les qualités des produits, ou celles nécessaires lors des réunions avec les clients, fournisseurs ou sous-traitants.

Le Code de la Propriété Intellectuelle (CPI) fournit aux entreprises les principaux moyens juridiques de protection de leur patrimoine. C'est le rôle de la propriété industrielle de protéger ce patrimoine résultant des efforts d'étude et de recherche et de l'expérience de l'entreprise. La propriété industrielle regroupe les brevets d'invention, les marques de fabrique, de commerce ou de service, et les dessins et modèles. Il s'agit de véritables titres de propriétés reconnus et protégés à l'échelle internationale qui fournissent à son détenteur un monopole d'exploitation.

C'est un moyen efficace pour lutter contre l'une des fins de l'espionnage : la contrefaçon. Déposer un brevet ou une marque peut dissuader d potentiels espions de pénétrer dans l'entreprise puisque l'information est rendue publique, mais verrouillée.

Cependant, ces instruments présentent certains inconvénients, et dans tous les cas ils s'avèrent insuffisants pour répondre à l'ensemble des besoins de sécurité de l'entreprise.

La protection industrielle concerne particulièrement la protection contre l'espionnage, qu'il soit privé ou d'État ; elle prend parfois le nom de contre-intelligence ou contre-espionnage privé. Dans ce domaine, vu le peu de recours juridiques, il s'agit davantage de changer les états d'esprit et les comportements de tout le personnel de l'entreprise que de vouloir faire de celle-ci un camp retranché.

Aujourd'hui un certain nombre d'industriels acceptent de transférer leur savoir-faire, en pariant sur leur capacité à garder une longueur d'avance. La France a signé nombre de contrats mirifiques avec la

Chine en décembre 2005 (Airbus pour la livraison de 150 avions A320, Eurocopter pour le développement conjoint d'un hélicoptère civil, Alcatel pour la fourniture d'un satellite de télécommunication, Total pour la création d'un réseau de stations-service dans la région de Shangaï,…). Mais en acceptant de transférer une partie de leur technologie dans l'empire du milieu, les industriels français « se tirent peut-être une balle dans le pied ». Car dans chaque succès commercial se cachent des concessions plus ou moins douloureuses. Areva, leader mondial du nucléaire civil et partenaire historique de la Chine s'est vu implicitement demander d'accompagner son offre de transferts de technologie, afin d'aider l'entreprise à emporter le marché. La question est de savoir si les importantes retombées financières valent bien ces compromis. C'est ce qu'a fait Alstom pour remporter un contrat de 17 milliards d'euros pour le TGV coréen, transférant une partie de son savoir-faire. « Les coréens ont joué très finement, écrit Ali Laïdi[16], et Alstom, trop focalisé sur l'énormité du contrat, n'a pas été assez vigilant sur les risques induits par le transfert de technologie ».
Pour mettre la main sur des brevets et autres informations confidentielles, faux stagiaires, faux appels d'offres pour obliger les entreprises à dévoiler leurs cartes et autres pratiques plus secrètes sont monnaies courantes. Ce qui pousse certains à penser qu'il est probablement préférable de vendre ce qui pourrait être obtenu de toute façon par des voies moins avouables.

b - L'organisation du contre-espionnage dans l'entreprise

Comme nous l'avons souligné, dans un contexte de confrontation, dont l'enjeu est la pérennité de l'entreprise, il s'agit d'affirmer sa position, de conquérir des marchés et de maîtriser les facteurs clés de succès ; mais il s'agit aussi de se prémunir contre les pratiques particulièrement agressives de certains concurrents qui se multiplient. Tous les moyens sont bons pour pirater, discréditer, déstabiliser, corrompre les acheteurs potentiels, saboter les essais, faire échouer les négociations ou encore dénoncer et attaquer les contrats.
Un exemple classique : une société conclut un marché portant sur la fourniture de matériels de pointe à très haute valeur ajoutée. Aussitôt d'invisibles mais bien réels agresseurs mettent en route une véritable machine de guerre destinée de toute évidence à faire capoter le contrat. Corruption, désinformation, témoignages providentiels sur la mauvaise qualité du produit proposé. Tout peut être envisagé pour discréditer une société qui a remporté un marché. Sans aller systématiquement jusqu'à ce type de situation, il n'en demeure pas moins que dans ce monde ouvert et complexe, la recherche du renseignement est permanente.

Étant donné l'importance de l'enjeu mais aussi la complexité du problème, il est clair que la sécurité ne peut être improvisée. Elle doit résulter d'une réflexion approfondie, au niveau global mais aussi sectoriel de l'entreprise. Les actions entreprises doivent être cohérentes et concerner aussi bien les

[16] Ali Laïdi - « Les secrets de la guerre économique » 2004

hommes que les biens. La sécurité dans l'entreprise est l'affaire de tous ; cependant, il est utile qu'elle soit orchestrée Après avoir identifié les menaces par leur nature, leur importance, leur probabilité d'occurrence, ce qui doit être protégé doit être recensé: les informations, les produits, les locaux, les hommes. Dans tous les cas, organiser la sécurité du patrimoine de l'entreprise doit se faire autour de trois axes : la responsabilisation du personnel, la protection des biens, et la surveillance de la communication. Il faut veiller à ce que chacun des ces principes soit effectivement appliqué à l'intérieur et à l'extérieur de l'entreprise.

2.6 - La protection offensive

a – La conservation du secret

La nouvelle donne politico-industrielle dans laquelle la France évolue actuellement, l'oblige à la fois à protéger ses intérêts franco-français, à s'ouvrir à l'Europe, et par conséquent à s'interroger sur ce qu'elle est prête à partager avec ses partenaires européens, et enfin, à conserver des liens étroits avec ses partenaires internationaux, en particulier les Américains, qui sont aussi des concurrents.

Quelle que soit la pondération retenue, il faut garder à l'esprit que par des moyens plus ou moins licites, de nombreuses informations sont recherchées ou convoitées par les concurrents. Outre les informations qui peuvent être « transmises » aux concurrents par simple méprise des règles élémentaires de sécurité (verrouiller son PC en quittant le bureau, discrétion dans les endroits publics,…), l'accélération de la globalisation des marchés conduit les entreprises à échanger et à partager de plus en plus d'informations, mais la plupart du temps sans un contrôle réel. A cela s'ajoute la vulnérabilité des systèmes d'information et de communication vis-à-vis des risques d'intrusion ou d'interception. Il convient également d'être extrêmement prudent sur les questions d'externalisation ou de sous-traitance, en particulier dans les secteurs très concentrés tels que ceux de la sécurité et de l'entretien (sociétés de gardiennage ou de nettoyage par exemple), ou des prestations intellectuelles (comme les cabinets d'audit ou de conseils, souvent d'origine anglo-saxonne). Le choix du prestataire demeure donc fondamental.

Tout cela renforce la légitimité des activités sécuritaires en termes de protection du patrimoine informationnel.

b - Piéger ses concurrents

Face à cette nécessité de protéger son patrimoine, et en optant pour une attitude offensive, plusieurs méthodes permettent de « piéger ses concurrents », dont la technique de déception. Celle-ci peut être définie comme représentant l'ensemble des mesures prises par une entreprise pour protéger son information stratégique, ce qui inclue toutes les manœuvres mises en place pour désinformer un tiers. Cela implique que l'on intègre les moyens que possède un tiers pour recueillir l'information nous concernant, c'est-à-dire la façon dont ce tiers pratique l'intelligence économique à nos dépends.

Parmi les mesures de déception, la plus connue est la désinformation, méthode évoquée en première partie. La désinformation peut revêtir différents aspects:

- L'exagération des dommages : ceci concerne en particulier les entreprises dont les activités ont une influence sur l'environnement et a fortiori les activités polluantes. (ex:campagnes contre les compagnies pétrolières ou les lignes haute tension d'EDF).
- La confusion entre la coïncidence et la causalité : ceci peut concerner une compagnie pharmaceutique dont un médicament sera accusé d'effets secondaires. (ex: campagne contre le Prozac).
- La primauté donnée aux risques relatifs sur les risques absolus : exemple du tabagisme passif.
- La manipulation des images : car on sait que la population est généralement très peu méfiante vis-à-vis des images, même quand des détails grossiers montrent qu'il y a contrefaçon.

c - L'utilisation d'agents d'influence

S'orienter dans le monde du changement et de l'instabilité, maîtriser son avenir, évoluer dans un environnement de plus en plus complexe, autant d'éléments qui nécessitent d'apprendre à manœuvrer avec des forces concurrentes, sinon hostiles, et trop puissantes pour être contrôlées. Le dirigeant doit donc disposer d'une lecture dynamique, car l'entreprise opère au sein d'un environnement qui ne cesse de se transformer.

Aussi pour éclairer et guider ses prises de décision, le chef d'entreprise nécessite d'un besoin d'informations et de relais ou d'agents d'influence. Les entreprises configurent donc des alliances pour déployer leur influence. Le réseau que peut développer une entreprise lui permet de s'ajuster avec flexibilité et vitesse pour manœuvrer sur les marchés ou activer les leviers d'influence.

Michael Porter[17] a cartographié les rapports de force entre les différents types d'acteurs :

- rivalité avec les concurrents,
- menace des nouveaux entrants,
- pouvoir de négociation des clients,
- menace des offres de substitution,
- pouvoir de négociation des fournisseurs, des distributeurs,…
- à quoi s'ajoutent les forces qui interfèrent sur le marché (interventions politiques, réglementaires et juridiques, l'évolution des matériaux, des procédés et technologies, les groupes de pression…).

Au sein de ce dispositif le dirigeant doit détecter les variables qui influencent l'évolution de manière favorable ou défavorable pour l'entreprise. De ce fait la surveillance de l'environnement ne peut pas être globale mais ciblée. Le rôle des agents d'influence prend ici toute son importance, car ils permettent à l'entreprise d'anticiper sur les événements qu'elle devra affronter.

---

[17] M Porter : « l'avantage concurrentiel » - 1986

3 - L'information « fermée », facteur de puissance

3.1 - Le lobbying, agent d'influence et de pouvoir

Au delà des techniques de veille réactives et proactives, on peut associer à l'intelligence stratégique des actions qui, par d'autres voies, visent les mêmes buts. Le lobbying est de ces actions. Il permet de mettre en place tout l'arsenal nécessaire pour valider la stratégie en vue de gagner le marché envisagé. Jean-Louis Levet[18] considère que les pratiques d'influence constituent l'une des quatre fonctions essentielles de l'intelligence économique.

Le lobbying doit faire gagner du temps, qu'il s'agisse d'éviter des retards ou d'anticiper sur les processus d'élaboration des décisions. Pour autant le lobbying détient une obligation de confidentialité propre. Il participe donc de l'importance des sources fermées. Avoir un bon carnet d'adresses signifie être capable à un moment précis de repérer le ou les décideurs sur le sujet donné, d'évaluer le contexte dans lequel ils seront amenés à prendre leur décision, éventuellement de leur transmettre une information au moment opportun. Certains sceptiques y voient un cinquième pouvoir, ce que réfute Dominique Prévot-Testart[19] : « le lobbying se distingue des quatre autres pouvoirs en ce qu'il procède de chacun d'entre eux. Il part d'une idée simple : laisser les professionnels intéressés évaluer et faire connaître les impacts des modifications législatives, réglementaires ou communautaires qui les concernent. »

Le lobbying vise à influencer l'évolution d'un secteur, dans le domaine légal, politique, syndical,… C'est une façon de faire qui tend à se développer en France et qui est employé ouvertement au sein des instances dirigeantes de l'Union européenne. Le lobbying s'est développé en France du fait de l'impact des décisions de la commission européenne sur la vie des affaires. L'objectif est de maitriser le risque de modification de la réglementation. A Bruxelles les groupes de lobby sont une source permanente d'informations. On estime qu'il y a 3000 groupes d'intérêt et 500 représentants d'entreprises, chargé de ce type de mission.
C'est une activité permettant une récolte fructueuse d'informations, plus souvent fermées qu'ouvertes, qui sont souvent données par certains responsables pour se faire « pardonner » de ne pas pouvoir être plus coopératifs. Ainsi, le lobbying américain, conjugué il est vrai avec un dollar faible, a enterré le

---

[18] Jean-Louis Levet, *L'intelligence économique, fondements méthodologiques d'une nouvelle démarche, Revue d'intelligence économique*, mars 1997

[19] D. Prévot-Testart - « Le lobbying ou l'échiquier des pouvoirs »

Rafale du groupe Dassault à Singapour. Compte-tenu de la qualité de la proposition française et de son adéquation aux critères techniques et opérationnels de l'appel d'offres, l'ouverture vers une autre source d'approvisionnement (sous-entendu autre qu'américaine) semblait possible. Ce qui n'a pas été le cas.

L'Etat et les pouvoirs publics deviennent en effet une cible importante sur le marché du renseignement. A tous les niveaux (européen, fédéral, régional, communautaire, provincial ou communal), le pouvoir politique fait l'objet d'interventions grandissantes, non seulement de la part de gouvernements étrangers, mais aussi de la part de secteurs industriels et professionnels privés qui, de groupes d'intérêt, se transforment en groupes de pression.
Comme l'intelligence économique, le lobbying se pratique aussi bien au sein qu'à l'extérieur de l'entreprise. Les possibilités d'influence et de lobbying des entreprises étant plus limitées que celles de l'Etat, il arrive donc que celles-ci s'adressent à des organismes officiels, à des ministères ou à des organismes internationaux pour défendre leurs intérêts, notamment au niveau de l'élaboration des normes.

Le lobbyiste est donc avant tout un courtier en information. Il doit bien connaître les processus politiques et sociaux, les procédures d'élaboration des décisions ainsi que les divers intervenants et leurs intérêts. Il doit pour cela connaître et fréquenter tous les intervenants et alliés possibles dans le jeu compliqué des systèmes d'influence : décideurs politiques, hauts fonctionnaires, syndicats, partis politiques, fédérations patronales, chambres de commerce, associations, groupes de pression, etc.
Bruxelles, siège des institutions de l'Union européenne, compte plusieurs centaines de groupes d'intérêts pratiquant un lobbying quotidien. Ces professionnels de l'influence observent, analysent et conseillent les entreprises désireuses d'infléchir la position des administrations préparant les futures normes industrielles, environnementales ou commerciales ; celles-ci sont en effet l'objet de négociations acharnées entre intérêts contradictoires.

Etudions le cas du programme américain d'avion de combat *Joint Strike Fighter* (JSF), emblématique de ces actions d'influence et de stratégie offensive.
Afin d'éviter que les principaux États producteurs européens ne lancent un programme d'avion de combat de nouvelle génération, concurrent du JSF, le département de la Défense américain a décidé d'ouvrir le programme JSF à la coopération internationale.
La promotion en faveur d'une participation au programme JSF s'est basée notamment sur une stratégie de communication mettant au premier plan les concepts de "partenariat véritable, d'influence et de confiance réciproque". Le Royaume-Uni, l'Italie et trois membres européens du "Club F-16", les Pays-Bas, la Norvège et le Danemark, ont répondu favorablement à l'appel américain. Le lobbying pour obtenir l'accord du parlement des Pays-Bas s'est avéré être particulièrement virulent.

Ainsi les Etats-Unis ont obtenu la participation d'industriels européens de premier plan au sein d'un projet industriel américain, ce qui représente sans conteste un obstacle pour la construction d'un avion de combat européen et tend simultanément à limiter les coûts du développement de ce projet pour les Etats-Unis.

A force de se manifester, les groupes de pression ont mis au point des démarches diverses pour obtenir avant les autres les précieuses informations, des techniques d'expression et de communication pour faire passer leur message et, parfois, pour prendre l'opinion à témoin[20].
Un rapport du commissaire européen de la Justice et des Affaires intérieures, daté du 2 juin 2003 et intitulé « une politique globale de l'Union européenne », indique que des « affaires ont montré qu'il pouvait exister des liens secrets entre les titulaires de fonctions publiques, le monde des affaires et des représentants des partenaires sociaux et d'autres groupes d'intérêt, au mépris des obligations légales, pour influencer des décisions politiques ou économiques importantes ».

Une des techniques les plus agressives mise en œuvre à des fins de lobbying et d'influence reste la guerre de l'information ou « l'*Info War* ». Il s'agit, pour une nation de défendre ses industries en diffusant un flot d'informations et/ou de désinformations déstabilisatrices envers les concurrents. Cette pratique peut également être utilisée comme nouvelle forme d'activisme par des groupes de pression ou par des ONG qui ont bien compris que le talon d'Achille des entreprises était leur image de marque.
De véritables campagnes de dénigrement peuvent parfois être mises en œuvre sur le réseau Internet et dans les médias pour attenter à la réputation d'un Etat, d'un secteur d'industrie ou d'activités, d'un concurrent, etc... Jean-Louis Levet décrit ainsi cette pratique d'influence : «La guerre de l'information est l'utilisation offensive de l'information afin d'affaiblir, de déstabiliser, ou détruire un adversaire »[21].

On le comprend, l'entreprise est devenue un acteur majeur de la géopolitique. La somme des jeux des acteurs que sont les entreprises n'est pas sans effet ni influence sur la situation géopolitique. L'entreprise subit les situations politiques internationales, mais elle agit aussi avec sa propre logique sur la scène mondiale. Les firmes internationales, elles, mettent en œuvre une diplomatie d'entreprise dont le lobbying est l'aspect le plus visible.

---

[20] Les débats à propos de la réglementation de la vente et de la publicité du tabac en ont été, pendant des années, une illustration.

[21] Jean-Louis Levet, *L'intelligence économique, fondements méthodologiques d'une nouvelle démarche, Revue d'intelligence économique*, mars 1997

Les entreprises étatiques, les Etats donc, n'hésitent pas à recourir à ces procédés d'influence, de lobbying pour défendre leur patrimoine. Cela apparaît aujourd'hui très clairement dans les cas d'offres publiques d'achat (OPA) de sociétés par des entreprises concurrentes étrangères.

3.2 - Fusions ou acquisitions imposées

Fusions et acquisitions peuvent être considérées, dans l'optique de notre étude, comme visant à éliminer un concurrent ou à s'approprier son savoir-faire, ses références de réalisations, ses listes de clients ou prospects, ses parts de marchés, etc.
Les fusions et acquisitions sont devenues une technique fort répandue chez les dirigeants des grandes entreprises. C'est un moyen facile d'éliminer un concurrent, d'augmenter artificiellement ses parts de marchés, d'attribuer de nouvelles stock options aux dirigeants, de plaire aux marchés boursiers, de faire gagner des fortunes aux firmes-conseil, de permettre aux gros actionnaires initiés de faire d'intéressants allers-retours boursiers, d'éliminer du personnel au cours des inévitables restructurations qui suivent, … mais aussi de s'emparer de ses savoir-faire, de sa technologie, de ses brevets…

La mondialisation de l'économie constitue une caractéristique nouvelle de notre société. Le pouvoir véritable est désormais détenu par un faisceau de groupes économiques planétaires et d'entreprises globales dont le poids dans les affaires du monde apparaît parfois plus important que celui des gouvernements et des Etats. Par ailleurs, ces restructurations industrielles et la globalisation des procédés au niveau mondial rendent plus difficile l'attribution d'une nationalité aux entreprises. C'est ainsi que des entreprises stratégiques pour le pays peuvent passer sous le contrôle d'investisseurs étrangers.
Les Etats-Unis ne sont pas, et de loin, le seul pays à faire de l'intelligence économique au sens large un outil au service de leurs puissances. Le Japon a eu historiquement une stratégie extrêmement offensive et soigneusement orchestrée. Puissance montante, la Chine n'est pas dépourvue non plus de stratégie, comme le sont la Russie et certains pays émergents. La guerre économique fait rage, c'est incontestable.
Comment déterminer dans ces conditions ce qui constitue le caractère national du potentiel économique ou scientifique à protéger ?
Quelles missions et quels moyens d'action un gouvernement peut-il donner à ses services de renseignement pour protéger le potentiel scientifique et économique de son pays ?

3.3 - Les investissements étrangers face à la notion de patrimoine économique

La loi française du 16 juillet 1980 réprime toute communication à une autorité publique étrangère, "de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public, précisés par l'autorité administrative en tant que de besoin". Selon l'article 410-1 du code pénal français de 1992, les intérêts fondamentaux de la Nation se caractérisent par : son indépendance, l'intégrité de son territoire, sa sécurité, la forme républicaine de ses institutions, les moyens de sa défense, sa diplomatie, la sauvegarde de sa population, l'équilibre de son milieu naturel et de son environnement, les éléments essentiels de son potentiel scientifique et économique et son patrimoine culturel.

Les dispositions du code monétaire et financier relatives aux investissements étrangers en France prévoient qu'un tel investissement doit faire l'objet d'une autorisation préalable de la direction du Trésor s'il « est de nature à mettre en cause l'ordre public, la sécurité publique ou encore la santé publique » ou bien s'il est « réalisé dans des activités de recherche, de production ou de commerce d'armes, de munitions, de poudres et substances explosives destinées à des fins militaires ou de matériels de guerre ». Le rapport du député Carayon[22] propose d'élargir ce système de contrôle aux «technologies de souveraineté et services de confiances».

Rendu public au mois de septembre 2003, ce document présente un panorama de l'intelligence économique en France et comporte trente-huit recommandations destinées à valoriser cette fonction. Selon le député rapporteur, l'Intelligence économique devrait être « une vraie et grande politique de l'Etat à l'instar de ce que sont les politiques de santé, d'environnement ou de fiscalité. » « Que cette politique soit nationale, décentralisée ou internationale, elle ne pourra s'épargner un effort de formation et d'information calibré à cette ambition et adapté à une certitude : l'intelligence économique est un patriotisme économique »,

Cette volonté aujourd'hui délibérée de contrer les offensives économiques étrangères n'est apparue qu'après de nombreux cas mettant en exergue les tentatives de conquête de secteurs stratégiques, les batailles d'influence, les tentatives de déstabilisation...Ainsi il arrive que des fonds d'investissement anglo-saxons prennent le contrôle d'entreprises française, peut-être dans une stricte logique économique ou parfois plus sûrement au service des intérêts de puissance de nations concurrentes. C'est le cas de l'affaire Gemplus, affaire désormais emblématique de la guerre économique.

[22] Rapport intitulé « Intelligence économique, compétitivité et cohésion sociale » et remis par le député Carayon au premier ministre en juillet 2003.

Gemplus :

L'histoire de Gemplus est devenue «le» cas d'école français et sert d'argument à tous les défenseurs d'une politique agressive en matière de renseignement économique[23]. Pour eux, le leader mondial de la carte à puce, fondé par Marc Lassus, a été la victime, entre 2000 et 2002, d'une tentative de démantèlement et de transfert de ses brevets aux Etats-Unis, par le biais d'un fonds d'investissement américain, Texas Pacific Group (TPG). Les Etats-Unis sont alors en retard en matière de cartes à puce, technologie dont les applications dans la sécurité sont devenues très sensibles. A l'invitation de Marc Lassus, l'arrivée de TPG au capital de Gemplus (en tant que premier actionnaire à hauteur de 26 %) a été suivie par la nomination d'un nouveau patron à la tête de ce fonds, Alex Mandl. Hors ce dernier se révèle être administrateur d'In-Q-Tel, le fonds d'investissement en nouvelles technologies créé par la CIA. Ce cas a été jugé suffisamment crédible pour nécessiter une intervention de la DST.

Carlyle – Arianespace :

Autre cas, celui de Carlyle – Arianespace. L'arrivée du fonds d'investissement Carlyle, réputé proche des milieux de la défense américains et de l'actuelle administration Bush, au sein d'Arianespace, pourrait nous amener à considérer que les Etats-Unis ont réussi à s'impliquer directement dans le lanceur européen. En prenant, en juillet 2003, le contrôle de 70 % du capital de l'industriel italien Fiat Avio (filiale de Finmeccanica), l'américain fait son entrée dans les plus importants programmes de l'industrie militaire et spatiale européenne (le futur avion de transport militaire A400M, l'avion de combat Eurofighter, Arianespace...). Le fonds d'investissement assure qu'il n'est là que pour des raisons financières. Les industriels et les politiques européens restent sceptiques. L'arrivée de Carlyle a suscité un appel du ministre de la Défense, Michèle Alliot-Marie, à la vigilance des intérêts français et européens.

Autant d'affaires qui posent la question de la maîtrise de technologies clés pour la sécurité nationale. La France, à l'inverse des Etats-Unis qui ont développé une doctrine de sécurité globale, reste dans une posture défensive. Toutefois, les appels au patriotisme économique augmentent depuis cette prise de conscience du danger que recouvre nos entreprises, considérées comme appartenant à des secteurs stratégiques. Face à la mondialisation, l'Etat doit se donner les moyens d'agir en développant un dispositif institutionnel, juridique et financier. L'appel au patriotisme économique du premier ministre Dominique de Villepin, lancé au lendemain des rumeurs de rachat de Danone par Pepsi, celui de président de la république Jacques Chirac lors de l'OPA faite par Mittal Steel sur Arcelor démontrent cette volonté de protéger au niveau étatique le patrimoine économique de la France, même si cette posture peut apparaître risquée sur le plan économique, car les autorités indiennes détiennent de

[23] C'est l'arrivée du fonds américain TPG dans Gemplus qui a convaincu le gouvernement français de confier au député Carayon sa mission sur l'intelligence économique.

considérables pouvoirs de nuisance contre les intérêts français en Inde. C'est bien une lutte d'Etat à Etat dont il s'agit, avec pour objectif l'acquisition de la puissance.

3.4 - Puissance immatérielle : une menace sur la souveraineté des Etats

On sait que la croissance des relations économiques internationales s'est accompagnée d'une forte montée en puissance des échanges de biens immatériels. Ce phénomène de dématérialisation du commerce mondial englobe les prestations de service transfrontières, les cessions de propriété industrielle et intellectuelle, les flux de technologie, et plus généralement les échanges virtuels. Cette dématérialisation des échanges a augmenté le champ de ce qu'on appelle les « produits sensibles ». Par la vente de licence, de franchise et par les accords de sous-traitance ou d'externalisation (*outsourcing*), les accords de compensation commerciale, le risque de transferts indésirables s'accroit. Les techniques modernes de commercialisation internationale sont génératrices de « fuites technologiques » involontaires.

Selon Bertrand Warusfel[24], la transformation profonde - due pour l'essentiel aux progrès techniques - que connaît notre société "modifie fondamentalement la valeur des principaux paramètres de l'équation du secret".
Selon lui, trois caractéristiques décrivent cette modernité :

- la diversification des facteurs de puissance qui tendent à devenir immatériels: à côté des facteurs traditionnels de la puissance politique, diplomatique et militaire, les enjeux de puissance et les luttes stratégiques se déplacent vers l'économie, la technologie et la culture, ce qui conduit à la prise en compte des secrets économiques, scientifiques et technologiques dans les mécanismes légaux de protection du secret;
- la diversification des acteurs de la puissance : à côté des Etats, les acteurs économiques, qu'ils soient nationaux ou supranationaux, jouent un rôle stratégique de plus en plus important;
- la transformation des lieux et des supports de la puissance : la nouvelle donne oppose la délocalisation de la puissance et l'immatérialité des ressources de l'information à l'ancien ordre basé sur la territorialité, la matérialité du pouvoir et l'appropriation physique des ressources. Les moyens et supports du secret sont aujourd'hui essentiellement des systèmes électroniques d'information vulnérables aux manipulations et aux techniques d'interception des communications.

[24] B. Warusfel : maître de conférences à la faculté de droit de Paris V, auteur d'une thèse sur la protection du secret.

Cette analyse montre bien tout le poids que l'immatériel prend aujourd'hui dans la notion de puissance. L'intervention des Etats pour protéger leur patrimoine économique démontre conjointement qu'ils se livrent à une nouvelle lutte, un nouveau conflit pour détenir la puissance qui relève désormais de l'aspect immatériel.

Conclusion

L'accroissement et le durcissement de la concurrence internationale soulignent chaque jour davantage les lacunes dans la déontologie des économies de marché. L'ampleur prise aujourd'hui par l'espionnage industriel est là pour le démontrer. A la lecture de ce bilan, il reste difficile de croire que les entreprises pourront lutter seules contre ces pratiques souterraines. Les instruments de protection à leur disposition sont bien maigres face à la détermination des espions.

L'instauration d'un dialogue entre les États apparaît comme une solution pour contenir les dérives à l'échelle mondiale. Dans un contexte économique qui voit resurgir les intérêts nationaux et individuels, une coordination de ce type risque de se heurter à de nombreuses difficultés. Qui pourra prétendre au rôle de médiateur ?

De même, la coopération de firmes de toutes nationalités pourrait aboutir à la mise au point d'un code de déontologie universelle. A l'image d'un traité, les entreprises signataires s'engagent à respecter les règles d'une course à l'information « loyale », où les pratiques illégales et immorales seraient abolies. Le développement d'une ingénierie de l'information, à travers les concepts de veille et d'intelligence économique, va dans cette voie, même si les définitions nécessitent encore d'être harmonisées.

A défaut de l'ouverture de tels dialogues à l'échelle mondiale, la guerre de l'ombre risque de s'amplifier. Les menaces économiques peuvent se répercuter sur la sphère politique. Dans ce cas, les délits d'espionnage industriels peuvent créer des tensions politiques, qui seraient préjudiciables à la paix mondiale.

Ce n'est qu'au prix d'un désarmement multilatéral, c'est-à-dire de l'abolition universelle de ces pratiques souterraines que le monde pourra prétendre au pacifisme économique.

TABLE DES MATIERES

INTRODUCTION 1

1 - LE TRAITEMENT DE L'INFORMATION, ENJEU DE LA GUERRE ECONOMIQUE 3

1.1 - Le rôle stratégique de l'information 3

1.2 - L'information, arme de domination économique 4

1.3 - Pouvoir et manipulation de l'information 5

1.4 – Capter l'information par un système de veille 6

1.5 - De l'intelligence économique à l'espionnage industriel 7

2 - L'ESPIONNAGE INDUSTRIEL OU L'ORGANISATION DU PILLAGE ECONOMIQUE 12

2.1 – Les fondements de l'espionnage industriel 12

2.2 – Moyens et procédés de l'espionnage industriel 13
a - Le recueil de l''information « grise » 14
b - Le recueil de l'information « noire » 15

2.3 - Les acteurs et les cibles 18
a- Les acteurs 18
b - Les cibles 19
c- Exemple d'une affaire récente : Messier - Dowty 21

2.4 - Des espions non inquiétés 22
- les risques de tensions diplomatiques 23
- les craintes dans le monde des affaires 23

2.5 - La protection du patrimoine de l'entreprise 24
a - Les armes de la propriété industrielle 24
b - L'organisation du contre-espionnage dans l'entreprise 25

2.6 - La protection offensive 26
a – La conservation du secret 26
b - Piéger ses concurrents 26
c - L'utilisation d'agents d'influence 27

3 - L'INFORMATION « FERMEE », FACTEUR DE PUISSANCE 28

3.1 - Le lobbying, agent d'influence et de pouvoir 28

3.2 - Fusions ou acquisitions imposées 31

3.3 - Les investissements étrangers face à la notion de patrimoine économique 32
Gemplus : 33
Carlyle – Arianespace : 33

3.4 - Puissance immatérielle : une menace sur la souveraineté des Etats 34

CONCLUSION **36**

BIBLIOGRAPHIE

Ouvrages

- COMMISSARIAT GENERAL DU PLAN. Intelligence économique et stratégie des entreprises. Rapport du groupe dirigé par Henri Martre. Paris : La DocumentationFrançaise, 1994.
- COMMISSARIAT GENERAL DU PLAN. Recherche et innovation : le temps des réseaux. Rapport du groupe « Recherche, technologie et compétitivité » dirigé par Guy Paillotin. Paris : La Documentation Française, 1993.
- COMMISSARIAT GENERAL DU PLAN. Information et compétitivité. Rapport du groupe présidé par René Mayer. Paris : La Documentation Française, 1990.
- ESSAMBERT Bernard. La guerre économique mondiale. Paris : Olivier Orban, 1991.
- HARBULOT Christian. La machine de guerre économique : Etats-Unis, Japon, Europe. Paris : Economica, 1992.
- HARBULOT Christian, « *La main invisible des puissances* », Paris, Ellipses, 2005.
- KLEIN Jean, BUFFOTOT Patrice, VILBOUX Nicole, (dir.) « *Vers une politique de sécurité et de défense* », Paris, Economica, 2003.
- LANDIER Augustin, THESMAR David, « *Quel patriotisme économique au XXIe siècle?* » Paris, Institut Montaigne, 2005.
- MARTINET B. MARTI Y-M. L'Intelligence économique : les yeux et les oreilles de l'entreprise. Paris : Les éditions d'organisation, 1995.
- PORTER Michael E. L'avantage concurrentiel des nations. Paris : InterEditions, 1993.
- ROUACH Daniel. La veille technologique et l'intelligence économique. Que Sais-je, n° 3086. Paris : Presses Universitaires de France, 1996.
- TOFFLER Alvin, « *Nouveaux pouvoirs : la violence, l'argent, le savoir* », Paris, Fayard, 1991.
- VERSAILLES David W., MERINDOL Valérie, CARDOT Patrice, « *La recherche et la technologie, Enjeux de puissance* », Paris, Economica, 2005.
- VILBOUX Nicole, *Les stratégies de puissance américaine*, Paris ; Ellipses (Repères stratégiques), 2002
- VILLAIN Jacques. L'entreprise aux aguets : information, surveillance de l'environnement, propriété et protection industrielles, espionnage et contre-

Articles de presse

- THREARD Yves, « *Actionnariat et patriotisme économique* », *Le Figaro*, 6 mars 2006.
- JUNGHANS Pascal, « *La Tribune s'est procurée la lettre de la Commission demandant des explications à la France sur la protection de secteurs sensibles* », *La Tribune*, 31 janvier 2006.
- DARRASON Olivier et VACCA Virginie, « *Patriotisme économique : il était temps* ! » *Défense Nationale*, novembre 2005.
- DELBECQUE Eric et LE GENTIL Colonel (er) Alain, « *De la sécurité globale à la sécurité des entreprises* », *Revue de la Défense Nationale*, novembre 2005.
- CORNEVIN Christophe, « *L'espionnage économique menace les PME* », Le Figaro économie, 30 novembre 2005
- ALLIOT-MARIE Michèle "*Patriotisme économique, pas une ligne Maginot*", Agence France Presse, 10 octobre 2005.
- ETCHEGOYEN Alain, « *Du patriotisme économique* », *Les Echos*, 27 septembre 2005.
- CEDRO Jean-Michel, « *Oncle Sam vise l'armement européen* », *Enjeux-Les Echos*, n°216, septembre 2005.
- LAÏDI Ali, « *Espionnage économique, arme cachée des grandes puissances* », Le monde diplomatique, mars 2005
- BISEAU Grégoire et CORI Nicolas, « *guerre économique : ère du soupçon dans les secteurs sensibles* », Libération, 24 novembre 2004
- JUILLET Alain, « *les secrets d'entreprise sont de plus en plus rares* », le Journal du Management – interview de monsieur Alain Juillet – septembre 2004.

Divers

- Dossier « *les armes de la guerre économique* », revue Problèmes économiques, 8 décembre 2004
- Dossier « *Intelligence économique ou renseignement* ? », *Revue de la défense Nationale*, décembre 2004.
- Colloque du groupe ESIEE "*de la concurrence à la guerre économique*" – 2 décembre 2004 (http://www.esiee.fr)
- Le rapport au Premier ministre de Bernard Carayon, « *Intelligence économique, compétitivité et cohésion sociale* », juin 2003
- « *Les Etats-Unis ont-ils commencé à mettre en place une stratégie de « containment» de la puissance européenne ? Si oui, laquelle ?* », Etude, CEIS, Août 2003.

- DESIRE Thibaud, « *La place du lobbying dans l'intelligence économique et stratégique française* », Cahier d'étude ESCP-EAP n°02-97, 2000
- VENZKE Ben N. « Economic/industrial espionage ». Intelligence watch report. 1996. (http://www.infowar.com)
- « *L'espionnage au service de la compétitivité* ». Coll : Le nouvel ordre économique. Paris : Masson ;1990.

Sites internet

www.ege.fr: Site de l'Ecole de guerre économique.
www.infoguerre.com: Site d'études en intelligence économique
www.bernard-carayon.fr: Site officiel du député et rapporteur
www.veille.com: Site d'intelligence économique.
www.finances.gouv.fr: Site du ministère des Finances
www.lesechos.fr
www.web2.latribune.fr/archiv.fr
www.intelligenceOnline.fr: lettre d'information
http://www.infowar.com